CLASSICAL CRYPTOSYSTEMS

Alphabet: {A,B,C,D,E,F,G,H,I,J,K,L,M,N,O,P,Q,R,S,T,U,V,W,X,Y,Z}

Numeral coding

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Standart form of the plaintext

A better, but more complicated method, for creating a grille method is to make up a set of master grille cards that have a number of hole punches in the same location on each card. Make sure you note which end is up on each of the card to ensure proper orientation

Plaintext in capitals with punctuation marks and spaces removed

ABETTERBUTMORECOMPLICATEDMETHODFORCREATINGAGRILLEMETHODISTOMAKEUPASETO
FMASTERGRILLECARDSTHATHAVEANUMBEROFHOLEPUNCHESINTHESAMELOCATIONONEACHC
ARDMAKESUREYOUNOTEWHICHENDISUPONEACHOFTHECARDTOENSUREPROPERORIENTATION

Plaintext written in groups of five letters

ABETT	ERBUT	MOREC	OMPLI	CATED	METHO
DFORC	REATI	NGAGR	ILLEM	ETHOD	ISTOM
AKEUP	ASETO	FMAST	ERGRI	LLECA	RDSTH
ATHAV	EANUM	BEROF	HOLEP	UNCHE	SINTH
ESAME	LOCAT	IONON	EACHC	ARDMA	KESUR
EYOUN	OTEWH	ICHEN	DISUP	ONEAC	HOFTH
ECARD	TOENS	UREPR	OPERO	RIENT	ATION

Encoded plaintext (p)

00 01 04 19 19	04 17 01 20 19	12 14 17 04 02	14 12 15 11 08	02 00 19 04 03	12 04 19 07 14
03 05 14 17 02	17 04 00 19 08	13 06 00 06 17	08 11 11 04 12	04 19 07 14 03	08 18 19 14 12
00 10 04 20 15	00 18 04 19 14	05 12 00 18 19	04 17 06 17 08	11 11 04 02 00	17 03 18 19 07
00 19 07 00 21	04 00 13 20 12	01 04 17 14 05	07 14 11 04 15	20 13 02 07 04	18 08 13 19 07
04 18 00 12 04	11 14 02 00 19	08 14 13 14 13	04 00 02 07 02	00 17 03 12 00	10 04 18 20 17
04 24 14 20 13	14 19 04 22 07	08 02 07 04 13	03 08 18 20 15	14 13 04 00 02	07 14 05 19 07
04 02 00 17 03	19 14 04 13 18	20 17 04 15 17	14 15 04 17 14	17 08 04 13 19	00 19 08 14 13

Frequencies and percetages of occurences of leters in the plaintext

A	19	9.05
B	3	1.43
C	11	5.24
D	7	3.33
E	29	13.81
F	4	1.90
G	3	1.43
H	12	5.71
I	11	5.24

J	0	0.00
K	2	0.95
L	7	3.33
M	9	4.29
N	12	5.71
O	20	9.52
P	6	2.86
Q	0	0.00
R	16	7.62

S	9	4.29
T	19	9.05
U	8	3.81
V	1	0.48
W	1	0.48
X	0	0.00
Y	1	0.48
Z	0	0.00

Statistical Information

Frequencies of the letters of the English alphabet:

High		Midde		Low	
	%		%		%
E	**12.31**	**L**	**4.03**	**B**	**1.62**
T	**9.59**	**D**	**3.65**	**G**	**1.61**
A	**8.05**	**C**	**3.20**	**V**	**.93**
O	**7.94**	**U**	**3.10**	**K**	**.52**
N	**7.19**	**P**	**2.29**	**Q**	**.20**
I	**7.18**	**F**	**2.28**	**X**	**.20**
S	**6.59**	**M**	**2.25**	**J**	**.10**
R	**6.03**	**W**	**2.03**	**Z**	**.09**
H	**5.14**	**Y**	**1.88**		

The most frequent letters in some languages:

ENGLISH		**GERMAN**		**FINNISH**		**FRENCH**		**ITALIAN**		**SPANISH**	
	%		%		%		%		%		%
E	12.31	E	18.46	A	12.06	E	15.87	E	11.79	E	13.15
T	9.59	N	11.42	I	10.59	A	9.42	A	11.74	A	12.69
A	8.05	I	8.02	T	9.76	I	8.41	I	11.28	O	9.49
O	7.94	R	7.14	N	8.64	S	7.90	O	9.83	S	7.60
N	7.19	S	7.04	E	8.11	T	7.26	N	6.88	N	6.95
I	7.18	A	5.38	S	7.83	N	7.15	L	6.51	R	6.25

Most frequent digrams in English

	%		%		%
TH	6.3	AR	2.0	HA	1.7
IN	3.1	EN	2.0	OU	1.4
ER	2.7	TI	2.0	IT	1.4
RE	2.5	TE	1.9	ES	1.4
AN	2.2	AT	1.8	ST	1.4
HE	2.2	ON	1.7	OR	1.4

Substitution Ciphers

A substitution cipher hides the message contents by replacing one symbol or a group of symbols with another. Then the main point is to determine a particular permutation of the alphabet or the set of blocks. Substitution ciphers can be classified as being *monoalphatic* or *polyalphabetic* and *monographic* or *polygraphic*.

A monoalphabetic substitution is a type of substitution in which each possible symbol is given a unique replacement symbol.In a polyalphabetic substitution, multiple distinct simple substitution alphabets are used. A monographic substitution encrypts a single letter at each step; where a polygraphic one maps two or more symbols to a group of symbols.

For defining arithmetic operations, the 26 letter alphabet is encoded as

```
 A  B  C  D  E  F  G  H  I  J  K  L  M
00 01 02 03 04 05 06 07 08 09 10 11 12

 N  O  P  Q  R  S  T  U  V  W  X  Y  Z
13 14 15 16 17 18 19 20 21 22 23 24 25
```

Shift Cipher
(Monoalphabetic / Monographic)

Ciphertext alphabet is obtained from the Plaintext alphabet by a shift transformation $f(c)=p+k$ Mod 26 with the Key k. Here x Mod 26 stands for the reaminder when x is divided by 26. Decryption uses the same transformation with the Key $-k$.

```
KEY: 3
PLAIN  ALPHABET: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
CIPHER ALPHABET: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
```

Plaintext:

```
BIRDS LOVEW HEATB READB ROWNR ICEAN DAWON DERFU LGRAI NCALL EDQUI NOA
```

Ciphertext:

```
ELUGV ORYHZ KHDWE UHDGE URZQU LFHDQ GDZRQ GHUIX OJUDL QFDOO HGTXL QRD
```

Shift Cipher (Monographic)

(Blocksize=1, calculations in $Z/26Z$))
$F(x)=x+a$
Key=a=7

Plaintext:

```
ABETTERBUTMORECOMPLICATEDMETHODFORCREATINGAGRILLEMETHODISTOMAKEUPASETO
FMASTERGRILLECARDSTHATHAVEANUMBEROFHOLEPUNCHESINTHESAMELOCATIONONEACHC
ARDMAKESUREYOUNOTEWHICHENDISUPONEACHOFTHECARDTOENSUREPROPERORIENTATION
```

Encoded ciphertext

```
0708112626  1124082700  1921241109  2119221815  0907001110  1911001421
1012212409  2411070015  2013071324  1518181119  1100142110  1525002119
0717112722  0725110021  1219072500  1124132415  1818110907  2410250014
0726140702  1107200119  0811242112  1421181122  0120091411  2515200014
1125071911  1821090700  1521202120  1107091409  0724101907  1711250124
1105210120  2100110314  1509141120  1015250122  2120110709  1421120014
1109072410  0021112025  0124112224  2122112421  2415112000  0700152120
```

Ciphertext

```
HILAA       LYIBA       TVYLJ       VTWSP       JHALK       TLAOV
KMVYJ       YLHAP       UNHNY       PSSLT       LAOVK       PZAVT
HRLBW       HZLAV       MTHZA       LYNYP       SSLJH       YKZAO
HAOHC       LHUBT       ILYVM       OVSLW       BUJOL       ZPUAO
LZHTL       SVJHA       PVUVU       LHJOJ       HYKTH       RLZBY
LFVBU       VALDO       PJOLU       KPZBW       VULHJ       OVMAO
LJHYK       AVLUZ       BYLWY       VWLYV       YPLUA       HAPVU
```

Most frequent letters of ciphertext

```
L=29  13.81%          V=20  9.52%
A=19   9.05%          H=19  9.05%
```

Cryptanalyst can easily suggest that E has mapped on L, V, A, or H, which give the respective Key values 7, 16, 22, or 3. Trying a=7, Plaintext can be obtained.

Shift Cipher (Monographic)

Plaintext

THEVE RTICE SOFFI VEPLA TONIC SOLID SGIVE THEON LYPER FECTL
YSYMM ETRIC ALDIS TRIBU TIONS OFPOI NTSON THESU RFACE OFASP
HERET HEREF OREIF NPOSI TIVEL YCHAR GEDPA RTICL ESARE CONST
RAINE DTOTH ESURF ACEOF ASPHE REAND NISNO TAPLA TONIC NUMBE
RTHEP ARTIC LESMU STHAV EANEQ UILIB RIUMC ONFIG URATI ONTHA
TISNO TPERF ECTLY SYMME TRICA LITTU RNSOU TTHAT EVENI FNISA
PLATO NICNU MBERT HEEQU ILIBR IUMCO NFIGU RATIO NISNO TNECE
SSARI LYTHE CORRE SPOND INGPL ATONI CSOLI DTHIS ARTIC LEDES
CRIBE SONEE QUILI BRIUM CONFI GURAT IONFO RVALU EOFNU PTOTH
IRTYT WO

Ciphertext

KYVMV IKZTV JFWWZ MVGCR KFEZT JFCZU JX1MV KYVFE CPGVI WVTKC
PJPDD VKIZT RCUZJ KIZSL KZFEJ FWGFZ EKJFE KYVJL IWRTV FWRJG
YVIVK YVIVW FIVZW EGFJZ KZMVC PTYRI XVUGR İKZTC VJRIV TFEJK
IRZEV UKFKY VJLIW RTVFW RJGYV IVREU EZJEF KRGCR KFEZT ELDSV
IKYVG RIKZT CVJDL JKYRM VREVH LZCZS IZLDT FEWZX LIRKZ FEKYR
KZJEF KGVİW VTKCP JPDDV KIZTR CZKKL IEJFL KKYRK VMVEZ WEZJR
GCRKF EZTEL DSVIK YVVHL ZCZSI ZLDTF EWZXL IRKZF EZJEF KEVTV
JJRIZ CPKYV TFIIV JGFEU ZEXGC RKFEZ TJFCZ UKYZJ RIKZT CVUVJ
TIZSV JFEVV HLZCZ SIZLD TFEWZ XLIRK ZFEWF IMRCL VFWEL GKFKY
ZIKPK NF

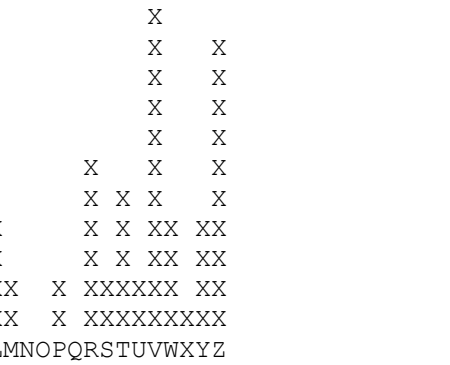
Enciphered using Shift Cipher.
Using the alphabetic Key 17
The length of the plain tex is 458 letters.

Plaintext alphabet is 26 Letters: A-Z.

Cipher Alphabet order:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
R S T U V W X Y Z A B C D E F G H I J K L M N O P Q

Frequency in above text: (Each X = 1%)



Shift Cipher (Digraphic)

(Blocksize=2, calculations in Z/676Z))
F(x)=x+a
Key=a=347

Plaintext

```
ABETTERBUTMORECOMPLICATEDMETHODFORCREATINGAGRILLEMETHODISTOMAKEUPASETO
FMASTERGRILLECARDSTHATHAVEANUMBEROFHOLEPUNCHESINTHESAMELOCATIONONEACHC
ARDMAKESUREYOUNOTEWHICHENDISUPONEACHOFTHECARDTOENSUREPROPERORIENTATION
```

Encryption

Plaintext in pairs	A B E T T E R B ...
Encoding	0001 0419 1904 1701 ...
26x+y	1 123 498 443 ...
Shifting (+347)	348 470 164 114 ...
Expreesing in base 26	1310 1802 0613 0410...
Decoding	N K S C G N E K...
Ciphertext	NKSCG NEK...

Ciphertext

```
NKSCG NEKIC ZXENP XZYYR PJGNQ VSCUX
QOCAQ ARJGR APNPE RYURV SCUXQ RGCBV
NTSDC JFNGX SVOBG NEPER YURLO ARBGQ
OCUJI NNWHV ONEXS QBURY HWPQS BVWGQ
SBNVR UBLOC VXAXA NNLUL OAQVN TSBIA
SHCDA XGNJQ VLUNA MWBHY BWRJP QBOGQ
RAOAR ABABA IARAE ACAEA EARAG AGABA
```

Shift Cipher (Hexagrapghic: Blocksize=6)

Plaintext

```
SINCETIMECANBEMEASUREDWITHEXTREMEPRECISIONANDSINCECISALSOKNOWNWITHGREATPRECIS
IONTHISRESULTSINANEXTREMELYACCURATEMEASUREMENTOFTHEDISTANCEBETWEENTHERADARANT
ENNAWHICHLAUNCHESTHEPULSEANDTHENEARESTPOINTONTHEPLANETWHICHREFLECTSITUNFORTUN
ATELYTHESTRENGTHOFTHERETURNINGECHODROPSOFFWITHTHEFOURTHPOWEROFDISTANCEANDSOTH
ISVERYACCURATETECHNIQUEISLIMITEDTOTHESOLARSYSTEMBUTITSEMPLOYMENTDOESMEANTHATA
LLSOLARSYSTEMDISTANCESAREKNOWNWITHGREATPRECISION
```

Key : 178455741 *(k)* Inverse Key: 130460035 *(-k)*
Mod : 308915776 *(m)*

Plaintext in blocks of 6:

```
SINCET IMECAN BEMEAS UREDWI THEXTR EMEPRE CISION ANDSIN CECISA LSOKNO WNWITH
GREATP RECISI ONTHIS RESULT SINANE XTREME LYACCU RATEME ASUREM
ENTOFT HEDIST ANCEBE TWEENT HERADA RANTEN NAWHIC HLAUNC HESTHE PULSEA
NDTHEN EAREST POINTO NTHEPL ANETWH ICHREF LECTSI TUNFOR TUNATE LYTHES
TRENGT HOFTHE RETURN INGECH ODROPS OFFWIT HTHEFO URTHPO WEROFD ISTANC
EANDSO THISVE RYACCU RATETE CHNIQU EISLIM ITEDTO THESOL ARSYST EMBUTI
TSEMPL OYMENT DOESME ANTHAT ALLSOL ARSYST EMDIST ANCESA REKNOW NWITHG REATPR
ECISIO N
```

Encoded Plaintext:

```
217750539 100606389  13922914 245469024 229031339  53090106  27740713   6005805  25631684 139173880
267723541  79127661 203852332 172618854 204141489 217749406 282256004 141663984 202320356   8588696
 53809749  85056159   5978574 235872981  85296406 202224841 154849502  88210228  85326934 187565768
156167609  47827487 184768208 163266569   6024415  96099593 132571512 235117913 235114650 142001358
233594003  89668206 204159215 101099915 168018856 168727123  91978056 245735192 263526565 103610860
 47756502 229098302 212952240 202320538  27195916  51505336 103806392 229027823   8101671  53040814
234050529 177520661  42124580   6279383   5232615   8101671  53067839   5979012 203996230 164665000
203824547  48592454 166339263
```

Encoded Ciphertext *(c=p+k (*mod *m)):*

```
 87290504 279062130 192378655 115008989  98571304 231545847 206196454 184461546 204087425   8713845
137263506 257583402  73392297  42158819  73681454  87289371 151795969  11203949  71860321 187044437
232265490 263511900 184434315 105412946 263752147  71764806  24389467 266665969 263782675  57105733
 25707574 226283228  54308173  32806534 184480156 274555334   2111477 104657878 104654615  11541323
103133968 268123947  73699180 279555656  37558821  38267088 270433797 115275157 133066530 282066601
226212243  98638267  82492205  71860503 205651657 229961077 282262133  98567788 186557412 231496555
103590494  47060626 220580321 184735124 183688356 186557412 231523580 184434753  73536195  34204965
 73364512 227048195  35879228
```

Ciphertext

```
HJALZC XMRLUW QEZNVB JRRNQR IHSHOA TMRZLN RJFSIW PNRCCW REPSMJ ATBUHX LOJSNQ
VRRKNY GEPSMR DOGRDB GFGEGC HJAKHN MUEOGN AYNLXD GBGOGN PTIAYV TOGYAC WEQSNC
PNPNVN IWROIC WFEJXJ GBBCYW CBJRCL WLOEHL WFGDBN EUZBYJ CEGQYW TBEONC EOVXNX
CTUOJU PNSDQQ XCVAYO AEQDMR IVAPJA IVAKNN AZGQZB IRRXBC WOTDBN GFHELW XNTNWQ
DEEYKB DFTGDC WTUNZX JSGRJX LFEXZM XTGKHL TBANMX IHWCPN GYNLXD GBGONN RIASLD
TJFVCV XTRNNX IHSCIU PSGINC TMPENR ISRWJU DYZOIC SOSCGN POGQVC PLZCIU PSGINC
TMQSNC PNPOMJ GEXXJF CWWDBP GEODKA TCWCCX DANJUI
```

Frequencies of letters in Ciphertext

```
             X
             X
  X          X
  X   X      X
  X X X      X   X     X
XXXXX X XX   XXX XXX  XX
XXXXX XXXX XXXXXXXXXXXXXX
XXXXXXXXXX XXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXX
ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

Affine Cipher
(Monoalphabetic / Monographic)

Ciphertext alphabet is obtained from the Plaintext alphabet by a transformation $F(c)=ap+b$ Mod 26 where the pair (a,b) is the Key. To have an invertible transformation one must have gcd(a,26)=1. Decryption uses the same transformation with the Key $(a^{-1},-a^{-1}b)$.

Key: (7,12)
Plain Alphabet: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Cipher Alphabet: M T A H O V C J Q X E L S Z G N U B I P W D K R Y F

Ciphertext:

TQBHI LGDOK JOMPT BOMHT BGKZB QAOMZ HMKGZ HOBVW LCBMQ ZAMLL OHUWQ ZGM

Affine Cipher (Monographic)

Plaintext

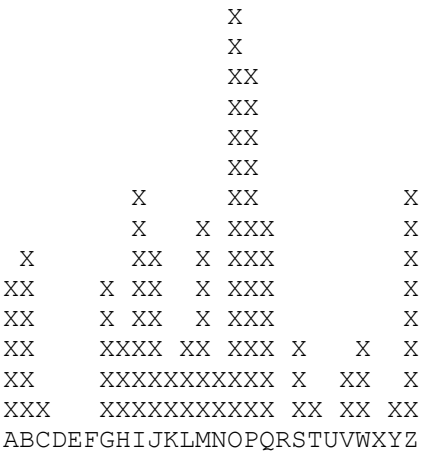
SINCETIMECANBEMEASUREDWITHEXTREMEPRECISIONANDSINCECISALSOKNOWNWITHGREATPRECIS
IONTHISRESULTSINANEXTREMELYACCURATEMEASUREMENTOFTHEDISTANCEBETWEENTHERADARANT
ENNAWHICHLAUNCHESTHEPULSEANDTHENEARESTPOINTONTHEPLANETWHICHREFLECTSITUNFORTUN
ATELYTHESTRENGTHOFTHERETURNINGECHODROPSOFFWITHTHEFOURTHPOWEROFDISTANCEANDSOTH
ISVERYACCURATETECHNIQUEISLIMITEDTOTHESOLARSYSTEMBUTITSEMPLOYMENTDOESMEANTHATA
LLSOLARSYSTEMDISTANCESAREKNOWNWITHGREATPRECISION

Key : 7,12 (a,b)
Inverse Key : 15,2 $(a^{-1},-a^{-1}b)$
Mod : 26

Ciphertext $(C=aP+b)$:

IQZAOPQSOAMZTOSOMIWBOHKQPJORPBOSONBOAQIQGZMZHIQZAOAQIMLIGEZGKZKQPJCBOMPNBOAQI
QGZPJQIBOIWLPIQZMZORPBOSOLYMAAWBMPOSOMIWBOSOZPGVPJOHQIPMZAOTOPKOOZPJOBMHMBMZP
OZZMKJQAJLMWZAJOIPJONWLIOMZHPJOZOMBOIPNGQZPGZPJONLMZOPKJQAJBOVLOAPIQPWZVGBPWZ
MPOLYPJOIPBOZCPJGVPJOBOPWBZQZCOAJGHBGNIGVVKQPJPJOVGWBPJNGKOBGVHQIPMZAOMZHIGPJ
QIDOBYMAAWBMPOPOAJZQUWOQILQSQPOHPGPJOIGLMBIYIPOSTWPQPIOSNLGYSOZPHGOISOMZPJMPM
LLIGLMBIYIPOSHQIPMZAOIMBOEZGKZKQPJCBOMPNBOAQIQGZ

Frequencies of letters in Ciphertext



Affine Cipher (Monographic)

Plaintext

THEVE RTICE SOFFI VEPLA TONIC SOLID SGIVE THEON LYPER FECTL
YSYMM ETRIC ALDIS TRIBU TIONS OFPOI NTSON THESU RFACE OFASP
HERET HEREF OREIF NPOSI TIVEL YCHAR GEDPA RTICL ESARE CONST
RAINE DTOTH ESURF ACEOF ASPHE REAND NISNO TAPLA TONIC NUMBE
RTHEP ARTIC LESMU STHAV EANEQ UILIB RIUMC ONFIG URATI ONTHA
TISNO TPERF ECTLY SYMME TRICA LITTU RNSOU TTHAT EVENI FNISA
PLATO NICNU MBERT HEEQU ILIBR IUMCO NFIGU RATIO NISNO TNECE
SSARI LYTHE CORRE SPOND INGPL ATONI CSOLI DTHIS ARTIC LEDES
CRIBE SONEE QUILI BRIUM CONFI GURAT IONFO RVALU EOFNU PTOTH
IRTYT WO

Ciphertext

WMDCD QWPXD THGGP CDKYR WHEPX THYPA TJPCD WMDHE YLKDQ GDXWY
LTLBB DWQPX RYAPT WQPUZ WPHET HGKHP EWTHE WMDTZ QGRXD HGRTK
MDQDW MDQDG HQDPG EKHTP WPCDY LXMRQ JDAKR QWPXY DTRQD XHETW
QRPED AWHWM DTZQG RXDHG RTKMD QDREA EPTEH WRKYR WHEPX EZBUD
QWMDK RQWPX YDTBZ TWMRC DREDN ZPYPU QPZBX HEGPJ ZQRWP HEWMR
WPTEH WKDQG DXWYL TLBBD WQPXR YPWWZ QETHZ WWMRW DCDEP GEPTR
KYRWH EPXEZ BUDQW MDDNZ PYPUQ PZBXH EGPJZ QRWPH EPTEH WEDXD
TTRQP YLWMD XHQQD TKHEA PEJKY RWHEP XTHYP AWMPT RQWPX YDADT
XQPUD THEDD NZPYP UQPZB XHEGP JZQRW PHEGH QCRYZ DHGEZ KWHWM
PQWLW FH

Enciphered using Shift Cipher.
Using the alphabetic Key 3,17
The length of the plain tex is 457 letters.

Plaintext alphabet is 26 Letters: A-Z.

Frequency in above text: (Each X = 1%)

```
   X           X
   X           X      X
   X           X      X
   X   X       X      X
   XX  X       XX     X
   XX  X       XXX X  X
   XX  X       XXX X  XX
   XX XX    X  XXX X  XXXX
   XX XX  X X  XXX X  XXXX
XXXXX XX  XXX  XXX XX XXXX
XXXXX XX XXXXX XXX XX XXXX
ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

Affine Cipher (Digraphic)

(Blocksize=2, calculations in Z/676Z))
F(x)=ax+b (a,676)=1
Key=a=413,b=517

Plaintext

ABETTERBUTMORECOMPLICATEDMETHODFORCREATINGAGRILLEMETHODISTOMAKEUPASETO
FMASTERGRILLECARDSTHATHAVEANUMBEROFHOLEPUNCHESINTHESAMELOCATIONONEACHC
ARDMAKESUREYOUNOTEWHICHENDISUPONEACHOFTHECARDTOENSUREPROPERORIENTATION

ENCRYPTION

Plaintextinpairs	A B E T T E R B ...
Encoding	0001 0419 1904 1701 ...
26x+y	1 123 498 443 ...
Transformation(413x+517)	254 616 11 280 ...
Expreesing in base 26	0920 2318 0011 1020...
Decoding	J U X S A L K U...
Ciphertext	JUXSA LKU...

Ciphertext

JUXSA LKUBS YHGLC HOEJZ NXALT NXSNH
MINYX YHXLZ YFLFR ZFQQN XSNHH ZHSMN
WTNPA XDLDH NNTVA LMFRZ FQNRD YKVWC
JSYXU LSKUN CLJHM CWQME KKVCH VUKWC
HVCNA QJRJS KHVHS LZRER DYTNW THVVY
ZDJPV HALNC BRKLC OVVQE CKHXV CFIWC
NRDYA SPLGV VYMEJ HMLJH RZGKO XLZCK

Affine Cipher (Hexagrapghic: Blocksize=6)

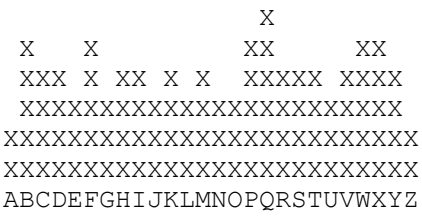
Plaintext

SINCETIMECANBEMEASUREDWITHEXTREMEPRECISIONANDSINCECISALSOKNOWNWITHGREATPRECIS
IONTHISRESULTSINANEXTREMELYACCURATEMEASUREMENTOFTHEDISTANCEBETWEENTHERADARANT
ENNAWHICHLAUNCHESTHEPULSEANDTHENEARESTPOINTONTHEPLANETWHICHREFLECTSITUNFORTUN
ATELYTHESTRENGTHOFTHERETURNINGECHODROPSOFFWITHTHEFOURTHPOWEROFDISTANCEANDSOTH
ISVERYACCURATETECHNIQUEISLIMITEDTOTHESOLARSYSTEMBUTITSEMPLOYMENTDOESMEANTHATA
LLSOLARSYSTEMDISTANCESAREKNOWNWITHGREATPRECISION

Key : 3164251,178455741 (a,b)
Inverse Key : 65265875,261251961 (a^{-1},$-a^{-1}b$)
Mod : 308915776

Ciphertext *(C=aP+b):*

ENKHRQNMBSTWEYBUZRAIACSBJZDCKSDFHHNFCPBIFWOMWWLWDLUHCJRFULCVYUNIZCBHVXSUQPENW
BKZPLRRMYQNKQOUDMRFFYIMSFAITQPPMJGMSFIRIMTXMSIRQQEJHXDQQIOFDFXTSVIQAZYXRJCUFL
PWKTRYEHOURQZHTFURXFYVLBQJXIVXPWRFKBDQHYTJWVEDHGMYESPLWCALJGWEAYMCWBRWKOPSGWI
OLFTWMBVRDUCOPQTWHRXFBTGKCWTLFDQCGJVCKRCFSXNQTRSXKVKGDGAVZCQEDGOYBKZHOMBXXVHO
UOJFUITQPPIVMKLFSCUGBPEWMCPXLBLTWVJPEWNYSBGHDQFTJXVBJXDYMYBLKVIQHPQYSFVWGSVQS
IXWNYSBGHDQBBHXDQCZKLCJPNXKVNKQATPDAWTWOSHKPXHVATPIYK



Simple Substitution Cipher
(Monoalphabetic / Monographic)

Arrangement of the Ciphertext alphabet is determined by a Keyword as follows. First, the letters of the Keyword is written without repetitions, then the unused letters of the alphabet are written in their usual ordering.

Key: LOVEBIRD

Plain Alphabet:	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Cipher Alphabet:	L O V E B I R D A C F G H J K M N P Q S T U W X Y Z

Ciphertext:

OAPEQ GKUBW DBLSO PBLEO PKWJP AVBLJ ELWKJ EBPIT GRPLA JVLGG BENTA JKL

To guarantee that no letter is mapped onto itself, sometimes the Keyword is used together with a letter. After arranging the cipher alphabet using the given word, it is rewritten starting from the given letter.

Key: LOVEBIRD,S

Plain Alphabet:	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Cipher Alphabet:	S T U W X Y Z L O V E B I R D A C F G H J K M N P Q

Ciphertext:

TOFWG BDKXM LXSHT FXSWT FDMRF OUXSR WSMDR WXFYJ BZFSO RUSBB XWCJO RDS

Simple Substitution Cipher

Plaintext:

THEVE RTICE SOFFI VEPLA TONIC SOLID SGIVE THEON LYPER FECTL
YSYMM ETRIC ALDIS TRIBU TIONS OFPOI NTSON THESU RFACE OFASP
HERET HEREF OREIF NPOSI TIVEL YCHAR GEDPA RTICL ESARE CONST
RAINE DTOTH ESURF ACEOF ASPHE REAND NISNO TAPLA TONIC NUMBE
RTHEP ARTIC LESMU STHAV EANEQ UILIB RIUMC ONFIG URATI ONTHA
TISNO TPERF ECTLY SYMME TRICA LITTU RNSOU TTHAT EVENI FNISA
PLATO NICNU MBERT HEEQU ILIBR IUMCO NFIGU RATIO NISNO TNECE
SSARI LYTHE CORRE SPOND INGPL ATONI CSOLI DTHIS ARTIC LEDES
CRIBE SONEE QUILI BRIUM CONFI GURAT IONFO RVALU EOFNU PTOTH
IRTYT WO

Ciphertext:

RQLAL HRVJL UMNNV ALOYG RMSVJ UMYVK UPVAL RQLMS YBOLH NLJRY
BUBZZ LRHVJ GYKVU RHVIF RVMSU MNOMV SRUMS RQLUF HNGJL MNGUO
QLHLR QLHLN MHLVN SOMUV RVALY BJQGH PLKOG HRVJY LUGHL JMSUR
HGVSL KRMRQ LUFHN GJLMN GUOQL HLGSK SVUSM RGOYG RMSVJ SFZIL
HRQLO GHRVJ YLUZF URQGA LGSLT FVYVI HVFZJ MSNVP FHGRV MSRQG
RVUSM ROLHN LJRYB UBZZL RHVJG YVRRF HSUMF RRQGR LALSV NSVUG
OYGRM SVJSF ZILHR QLLTF VYVIH VFZJM SNVPF HGRVM SVUSM RSLJL
UUGHV YBRQL JMHHL UOMSK VSPOY GRMSV JUMYV KRQVU GHRVJ YLKLU
JHVIL UMSLL TFVYV IHVFZ JMSNV PFHGR VMSNM HAGYF LMNSF ORMRQ
VHRBR CM

Enciphered using 'Simple substitution cipher'.
Using the alphabetic Key:
Plaintext Key: 'G'
Ciphertext Key: 'SMOOTHSURFACE','P'
The length of the plain tex is 457 letters.
Plaintext alphabet is 26 Letters: A-Z.
Substitution alphabet (Keyd Mix):
Plaintext Alphabet: G H I J K L M N O P Q R S T U V W X Y Z A B C D E F
Ciphertext Alphabet: P Q V W X Y Z S M O T H U R F A C E B D G I J K L N

Generation Of The Mixed Ciphertext Alphabet:
Precede By Key:
S M O _ T H _ U R F A C E _ B _ D _ _ G _ I J K L _ N _ P Q _ _ _ _ V W X Y Z

Frequency in above text: (Each X = 1%)

```
            X          X
            X      X   X
            X      X   X
            XX     X   X
          X   XX     XX  X
        XX    XX     XX XX
        XX X XX      XX XX
      XXX X XXX   XXX XX  X
      XXX X XXXX XXX XX   X
XX    XXXXXXXXXX XXX XX   XX
XX    XXXXXXXXXXXXXXXXX   XX
ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

Vigenere Cipher (Repetitive Key)
(Polyalphabetic / Monographic)

The Keyword is written repeatedly below the Plaintext and corresponding letters are added modulo 26.

Key: LOVEBIRD

```
BIRDS LOVEW HEATB READB ROWNR ICEAN DAWON DERFU LGRAI NCALL EDQUI NOA
LOVEB IRDLO VEBIR DLOVE BIRDL OVEBI RDLOV EBIRD LOVEB IRDLO VEBIR DLO
```

Ciphertext:
```
MWMHT TFYPK CIBBS UPOYF SWNQC WXIBV UDHCI HFZWX WUMEJ VTDWZ ZHRCZ QZO
```

Vigenere Cipher (Progressive Key)
(Polyalphabetic / Monographic)

Same as the Vigenere repetitive Key cipher with only difference, the letters of the Key is shifted by 1 at each repetition.

```
BIRDS LOVEW HEATB READB ROWNR ICEAN DAWON DERFU LGRAI NCALL EDQUI NOA
LOVEB IRDMP WFCJS ENQXG DKTFO RYHEL UGPSZ IFMVH QTAJG NWIRU BKHOX JSV
```

Ciphertext:
```
MWMHT TFYQL DJCCT VRQAH UYPSF ZALEY XGLGM LJDAB BZRJO AYICF FNXIF WGV
```

Vigenere Cipher (Autoclave)
(Polyalphabetic / Monographic)

Same as the Vigenere repetitive Key cipher with only difference, the Key is used only once then it is followed by the Plaintext.

Key: LOVEBIRD

```
BIRDS LOVEW HEATB READB ROWNR ICEAN DAWON DERFU LGRAI NCALL EDQUI NOA
LOVEB IRDBI RDSLO VEWHE ATBRE ADBRO WNRIC EANDA WONDE RFULG RAINC ALL
```

Ciphertext:
```
MWMHT TFYFE YHSEP MIWKF RHXEV IFFRB ZNNWP HEEIU HUEDM EHUWR VDYHK NZL
```

Vigenere Cipher (Key+Ciphertext)
(Polyalphabetic / Monographic)

Same as the autoclave mode but the Key is followed by the Ciphertext.

Key: LOVEBIRD

```
BIRDS LOVEW HEATB READB ROWNR ICEAN DAWON DERFU LGRAI NCALL EDQUI NOA
LOVEB IRDMW MHTTF YQSTL TMGPU SWMKA CCLAY QKNFC HOLTO EKWSU CTWRM WDF
```

Ciphertext:
```
MWMHT TFYQS TLTMG PUSWM KACCL AYQKN FCHOL TOEKW SUCTW RMWDF GWMLU JRF
```

Vigenere (Repetitive Key)

Keyword:SCIENCE

```
P ABETT ERBUT MOREC OMPLI CATED METHO DFORC REATI NGAGR ILLEM ETHOD ISTOM
K SCIEN CESCI ENCES CIENC ESCIE NCESC IENCE SCIEN CESCI ENCES CIENC ESCIE
+ SDMXG GVTWB QBTIU QUTYK GSVMH ZGXZQ LJBTG JGIXV PKSIZ MYNIE GBLBF MKVWQ

P AKEUP ASETO FMAST ERGRI LLECA RDSTH ATHAV EANUM BEROF HOLEP UNCHE SINTH
K NCESC IENCE SCIEN CESCI ENCES CIENC ESCIE NCESC IENCE SCIEN CESCI ENCES
+ NMIMR IWRVS XOIWG GVYTQ PYGGS TLWGJ ELJIZ RCRMO JIEQJ ZQTIC WRUJM WVPXZ

P ESAME LOCAT IONON EACHC ARDMA KESUR EYOUN OTEWH ICHEN DISUP ONEAC HOFTH
K CIENC ESCIE NCESC IENCE SCIEN CESCI ENCES CIENC ESCIE NCESC IENCE SCIEN
+ GAEZG PGEIX VQRGP MEPJG STLQN MIKWZ ILQYF QBIJJ MUJMR QKWMR WRRCG ZQNXU

P ECARD TOENS UREPR OPERO RIENT ATION
K CESCI ENCES CIENC ESCIE NCESC IENCE
+ GGSTL XBGRK WZICT SHGZS EKIFV IXVQR
```

Ciphertext

```
SDMXG GVTWB QBTIU QUTYK GSVMH ZGXZQ
LJBTG JGIXV PKSIZ MYNIE GBLBF MKVWQ
NMIMR IWRVS XOIWG GVYTQ PYGGS TLWGJ
ELJIZ RCRMO JIEQJ ZQTIC WRUJM WVPXZ
GAEZG PGEIX VQRGP MEPJG STLQN MIKWZ
ILQYF QBIJJ MUJMR QKWMR WRRCG ZQNXU
GGSTL XBGRK WZICT SHGZS EKIFV IXVQR
```

Vigenere (Autoclave)

Plaintext	ABETT ERBUT MOREC OMPLI CATED METHO DFORC REATI NGAGR ILLEM ETHOD ISTOM AKEUP ASETO FMAST ERGRI LLECA RDSTH ATHAV EANUM BEROF HOLEP UNCHE SINTH ESAME LOCAT IONON EACHC ARDMA KESUR EYOUN OTEWH ICHEN DISUP ONEAC HOFTH ECARD TOENS UREPR OPERO RIENT ATION
Key	SCIEN CEABE TTERB UTMOR ECOMP LICAT EDMET HODFO RCREA TINGA GRILL EMETH ODIST OMAKE UPASE TOFMA STERG RILLE CARDS THATH AVEAN UMBER OFHOL EPUNC HESIN THESA MELOC ATION ONEAC HCARD MAKES UREYO UNOTE WHICH ENDIS UPONE ACHOF THECA RDTOE NSURE PROPE RORIE
Ciphertext	SDMXG GVBVX FHVVD IFBZZ GCHQS XMVHH HIAVV YSDYW EIRKR BTYKM KKPZO MEXHT ONMMI OEEDS ZBAKX XFLDI DEITG ILDEL CTYDN XHNNT BZVOS BAMIG ISJVP WXHGJ LWSUR EVGST USYCP ETKVP OEHMC RGSLU QYYYF IKIUV CPVXR ZPAWW SAHIU BDTGL EEHFI MVIPS LUXDV BHYIS GZSCX RHZWR

Vigenere (Key+C)

Plaintext	ABETT ERBUT MOREC OMPLI CATED METHO DFORC REATI NGAGR ILLEM ETHOD ISTOM AKEUP ASETO FMAST ERGRI LLECA RDSTH ATHAV EANUM BEROF HOLEP UNCHE SINTH ESAME LOCAT IONON EACHC ARDMA KESUR EYOUN OTEWH ICHEN DISUP ONEAC HOFTH ECARD TOENS UREPR OPERO RIENT ATION
Key	SCIEN CESDM XGGVT XFJUX ZVLRY FFBVE QBRJU CSTGF AWTWT ZNNCT CKHYY GFGDO MBOXZ RAMLS RORSQ EGWAR KJIXC RZVUM ZCICN NTZVP CIRTM PBDMI HRWPO QXBEY WSIFO XFAKI RSITC KBZGV HPOBB NXHGR NBXBZ AIRZL VMOBV VSDOV FIYAV IKTVC AXPYY OJEZP PBHXI MHJSL MZAWN JZDHE
Ciphertext	SDMXG GVTXF JUXZV LRYFF BVEQB RJUCS TGFAW TWTZN NCTCK HYYGF GDOMB OXZRA MLSRO RSQEG WARKJ IXCRZ VUMZC ICNNT ZVPCI RTMPB DMIHR WPOQX BEYWS IFOXF AKIRS ITCKB ZGVHP OBBNX HGRNB XBZAI RZLVM OBVVS DOVFI YAVIK TVCAX PYYOJ EZPPB HXIMH JSLMZ AWNJZ DHEJG JSLVR

Vigenere

Plaintext

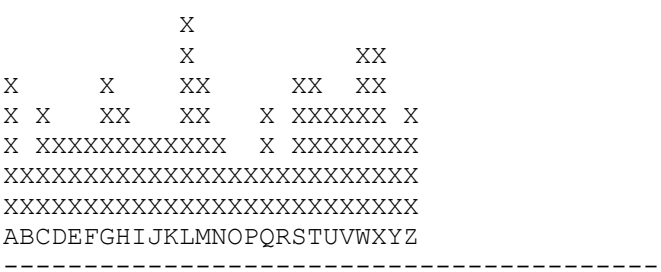
```
THEVE RTICE SOFFI VEPLA TONIC SOLID SGIVE THEON LYPER FECTL
YSYMM ETRIC ALDIS TRIBU TIONS OFPOI NTSON THESU RFACE OFASP
HERET HEREF OREIF NPOSI TIVEL YCHAR GEDPA RTICL ESARE CONST
RAINE DTOTH ESURF ACEOF ASPHE REAND NISNO TAPLA TONIC NUMBE
RTHEP ARTIC LESMU STHAV EANEQ UILIB RIUMC ONFIG URATI ONTHA
TISNO TPERF ECTLY SYMME TRICA LITTU RNSOU TTHAT EVENI FNISA
PLATO NICNU MBERT HEEQU ILIBR IUMCO NFIGU RATIO NISNO TNECE
SSARI LYTHE CORRE SPOND INGPL ATONI CSOLI DTHIS ARTIC LEDES
CRIBE SONEE QUILI BRIUM CONFI GURAT IONFO RVALU EOFNU PTOTH
IRTYT WO
```

Ciphertext:

```
LTSJX YLCTJ SQJXU JSISS NFSIE WGXWR LNAPV YHGSF XMDXY XYTYL
AWQYA SMYAW RQDKW LDWPN AAIEX OHTGU BHLVF NYJSW VXMQS HMSMG
METIL TSFXM GLVNF PTGEW HBCWF PHHCV YQRDT YLCTQ EUEJQ QCGZL
LRNNG HLAHV XZMLW FCGSX MGDAL JYRSD PMKZC HTWDU KTNKG FGAPX
YLBVU ATXAO ZSLTM MKMAX ISZSE NPDCS WIWQU ABTBN MLRYI QRLTO
HBZFI KUETJ WOHZR ZQGDJ TTMUM ZWMAM LEXOW XLTOH XCWHZ KNKWS
BZOMV FCTSU OFWDH VXLIO ZQIDV AGAQH UXCXZ RCXAA BWLUG NEJCG
WKMFW EFLBV HOTVW EDCGK AHXUL CXGZW QLVDC UYHKW SDHWV SWXVX
CTMTQ GCGLW KLNLK FJUIA VVFZZ LUTEL UCBYV JPRQU GSXZI DMVLB
ZWTAX OA
```

Enciphered using 'Vigenere cipher'.
Using the alphabetic Key `'SMOOTHSURFACE'`.
The length of the plain tex is 457 letters.
Plaintext alphabet is 26 Letters: `A-Z`.
Operation Mode:Repetitive Key

Frequency in above text: (Each X = 1%)



Kasiski Analysis

It is given that the following Ciphertext is obtained by Keyword Vigenere cryptosystem.

```
SDMXG GVTWB QBTIU QUTYK GSVMH ZGXZQ LJBTG JGIXV PKSIZ MYNIE GBLBF
MKVWQ NMIMR IWRVS XOIWG GVYTQ PYGGS TLWGJ ELJIZ RCRMO JIEQJ ZQTIC
WRUJM WVPXZ GAEZG PGEIX VQRGP MEPJG STLQN MIKWZ ILQYF QBIJJ MUJMR
QKWMR WRRCG ZQNXU GGSTL XBGRK WZICT SHGZS EKIFV IXVQR
```

Most frequent triples and quadrapules are as follows:

```
GGV:2/ 70        STL:3/ 56,42        QNMI:2/ 84
IXV:3/ 91,77     UJM:2/ 49           GGST:2/ 98
QNM:2/ 84        XVQ:2/ 77           GSTL:3/ 56,42
NMI:2/ 84        VQR:2/ 77           IXVQ:2/ 77
GGS:2/ 98        KWZ:2/ 42           XVQR:2/ 77
GST:3/ 56,42     WZI:2/ 42           KWZI:2/ 42
```

One can easily suggest that the Key length is 7. Then we rewrite the Ciphertext in 7 columns. We also write the most frequent letter in each column.:

S	D	M	X	G	G	V
T	W	B	Q	B	T	I
U	Q	U	T	Y	K	G
S	V	M	H	Z	G	X
Z	Q	L	J	B	T	G
J	G	I	X	V	P	K
S	I	Z	M	Y	N	I
E	G	B	L	B	F	M
K	V	W	Q	N	M	I
M	R	I	W	R	V	S
X	O	I	W	G	G	V
Y	T	Q	P	Y	G	G
S	T	L	W	G	J	E
L	J	I	Z	R	C	R
M	O	J	I	E	Q	J
Z	Q	T	I	C	W	R
U	J	M	W	V	P	X
Z	G	A	E	Z	G	P
G	E	I	X	V	Q	R
G	P	M	E	P	J	G
S	T	L	Q	N	M	I
K	W	Z	I	L	Q	Y
F	Q	B	I	J	J	M
U	J	M	R	Q	K	W
M	R	W	R	R	C	G
Z	Q	N	X	U	G	G
S	T	L	X	B	G	R
K	W	Z	I	C	T	S
H	G	Z	S	E	K	I
F	V	I	X	V	Q	R
S	Q	I	X	B	G	G
				V		

Since the most frequent letters in English are E, T, A, and O, we first consider the case he above letters are images of these letters.
For example, if E is mapped to S in the first column, then the first letter of the Key must be O.
Considering all possibilities we get the following table:

Most Frequent Letter in the column	S	Q	I	X		G	G
Letter of the Key if preimage is E	O	M	E	T		C	C
Letter of the Key if preimage is T	Z	X	P	E		J	J
Letter of the Key if preimage is A	S	Q	I	X		G	G
Letter of the Key if preimage is O	E	C	U	J		S	S

Among all these letters, the G in 6th column repeats 7 times. So we start by assuming that the 6th letter of the Key is C. Then the 6th column of the Plaintext is

					C	
S	D	M	X	G	**E**	V
T	W	B	Q	B	**R**	I
U	Q	U	T	Y	**I**	G
S	V	M	H	Z	**E**	X
Z	Q	L	J	B	**R**	G
J	G	I	X	V	**N**	K
S	I	Z	M	Y	**L**	I
E	G	B	L	B	**D**	M
K	V	W	Q	N	**K**	I
M	R	I	W	R	**T**	S
X	O	I	W	G	**E**	V
Y	T	Q	P	Y	**E**	G
S	T	L	W	G	**H**	E
L	J	I	Z	R	**A**	R
M	O	J	I	E	**O**	J
Z	Q	T	I	C	**U**	R
U	J	M	W	V	**N**	X
Z	G	A	E	Z	**E**	P
G	E	I	X	V	**O**	R
G	P	M	E	P	**H**	G
S	T	L	Q	N	**K**	I
K	W	Z	I	L	**O**	Y
F	Q	B	I	J	**H**	M
U	J	M	R	Q	**I**	W
M	R	W	R	R	**A**	G
Z	Q	N	X	U	**E**	G
S	T	L	X	B	**E**	R
K	W	Z	I	C	**R**	S
H	G	Z	S	E	**I**	I
F	V	I	X	V	**O**	R

Last letter of Key, most probably, is not C. So we may try replacing I and R, each of which appears five times in the last row, with E. Replacing I with E gives RE, LE, LE, KE, IE and replacing R with E gives AE, UE, OE, EE, OE. It seems reasonable to replace I with E which means that the last letter of the Key is E. Then, we get

					C	E
S	D	M	X	G	**E**	**R**
T	W	B	Q	B	**R**	**E**
U	Q	U	T	Y	**I**	**C**
S	V	M	H	Z	**E**	**T**
Z	Q	L	J	B	**R**	**C**
J	G	I	X	V	**N**	**G**
S	I	Z	M	Y	**L**	**E**
E	G	B	L	B	**D**	**I**
K	V	W	Q	N	**K**	**E**
M	R	I	W	R	**T**	**O**
X	O	I	W	G	**E**	**R**
Y	T	Q	P	Y	**E**	**C**
S	T	L	W	G	**H**	**A**
L	J	I	Z	R	**A**	**N**
M	O	J	I	E	**O**	**F**
Z	Q	T	I	C	**U**	**N**
U	J	M	W	V	**N**	**T**
Z	G	A	E	Z	**E**	**L**
G	E	I	X	V	**O**	**N**
G	P	M	E	P	**H**	**C**
S	T	L	Q	N	**K**	**E**
K	W	Z	I	L	**O**	**U**
F	Q	B	I	J	**H**	**I**
U	J	M	R	Q	**I**	**S**
M	R	W	R	R	**A**	**C**
Z	Q	N	X	U	**E**	**C**
S	T	L	X	B	**E**	**N**
K	W	Z	I	C	**R**	**O**
H	G	Z	S	E	**I**	**E**
F	V	I	X	V	**O**	**N**

There are four V in the 5th column and they stand as vNG, vNT, vON. So, it most be a vowel. Possibilities are ANG ANT AON, ENG ENT EON, ING INT ION, ONG ONT OON, UNG UNT UON. It is reasonable to try replacing V with I which means that the 5th letter of the Key is N:
Moreover we have two I's in the third column and two X's in the fourth column preceding vON (ION) so I must correspond to A and X must correspond T. This means that the third letter is I and fourth letter is E. Then with this substitutions we have

		I	E	N	C	E
S	D	**E**	**T**	**T**	**E**	**R**
T	W	**T**	**M**	**O**	**R**	**E**
U	Q	**M**	**P**	**L**	**I**	**C**
S	V	**E**	**D**	**M**	**E**	**T**
Z	Q	**D**	**F**	**O**	**R**	**C**
J	G	**A**	**T**	**I**	**N**	**G**
S	I	**R**	**I**	**L**	**L**	**E**
E	G	**T**	**H**	**O**	**D**	**I**
K	V	**O**	**M**	**A**	**K**	**E**
M	R	**A**	**S**	**E**	**T**	**O**
X	O	**A**	**S**	**T**	**E**	**R**
Y	T	**I**	**L**	**L**	**E**	**C**
S	T	**D**	**S**	**T**	**H**	**A**
L	J	**A**	**V**	**E**	**A**	**N**
M	O	**B**	**E**	**R**	**O**	**F**
Z	Q	**L**	**E**	**P**	**U**	**N**
U	J	**E**	**S**	**I**	**N**	**T**

Z G **S A M E L**
G E **A T I O N**
G P **E A C H C**
S T **D M A K E**
K W **R E Y O U**
F Q **T E W H I**
U J **E N D I S**
M R **O N E A C**
Z Q **F T H E C**
S T **D T O E N**
K W **R E P R O**
H G **R O R I E**
F V **A T I O N**

Now, considering the frequency table above, we can suggest that the Key is SCIENCE, which gives the Plaintext:

A better, but more complicated method, for creating a grille method is to make up a set of master grille cards that have a number of hole punches in the same location on each card. Make sure you note which end is up on each of the card to ensure proper orientation.

One-Time Pad

Plaintext

```
SINCETIMECANBEMEASUREDWITHEXTREMEPRECISIONANDSINCECISALSOKNOWNWITHGREA
TPRECISIONTHISRESULTSINANEXTREMELYACCURATEMEASUREMENTOFTHEDISTANCEBETW
EENTHERADARANTENNAWHICHLAUNCHESTHEPULSEANDTHENEARESTPOINTONTHEPLANETWH
ICHREFLECTSITUNFORTUNATELYTHESTRENGTHOFTHERETURNINGECHODROPSOFFWITHTHE
FOURTHPOWEROFDISTANCEANDSOTHISVERYACCURATETECHNIQUEISLIMITEDTOTHESOLAR
SYSTEMBUTITSEMPLOYMENTDOESMEANTHATALLSOLARSYSTEMDISTANCESAREKNOWNWITHG
REATPRECISIONZZZZZZZZZZ
```

Key

```
MANYPEOPLETHINKLOVEBIRDSARENOTPARROTSBUTTHEYARETHEYAREANAFRICANSPECIES(THEREA
RENINESPECIESOFLOVEBIRDS)ANDTHEYHAVEALLTHETELLTALECHARACTERISTICSFROMTHEHOOKE
DBILLTOTHETWOTOESFORWARDTWOTOESBACKLOVEBIRDSHAVETHEABILITYTOMIMICASALLPARROTS
DOBUTTHEYARENTASWELLKNOWNFORTHISLOVEBIRDSAREONEOFTHECUDDLIESTANDMOSTPLAYFULPA
RROTSWHENTHEYAREHANDFEDANDPROPERLYSOCIALIZEDWERAISEAFEWSELECTCOLORMUTATIONSOF
PEACHFACEDLOVEBIRDSHANDRAISINGTHEMTOBETHEBESTPETSPOSSIBLESO
```

Ciphertext

```
EIAATXWBPGTUJRWPONYSMUZATYIKHKTMVGFXUJMBHUELDJMGJIAIJELFOPEWYNJAILIZISUIYITMS
ZSABUMKGIUCPLGNYOIIYBIHEGLLDVJYPHTZQELDNYIFIYEHFELGKIJTCGGVJWMEGWSKVQKHHHFOXX
HOVLHAWVOPTQBVVIKYVVLUCVXWBWHLWOECBPGOTPQEWGUTCIISENFBHPBAAFQNXMETKIEFCFFIHNF
DHFFRMOIQTIIAZTZKJESOESPHWBZGNMUSCYVPXJRXFNMHUXVJYVYTNKSZEIJHFQLEHSGRPALIMZIH
ZJJXJUHGPNYEREKIJHALVYHIFOXDWIIUEMLVGAOWIQWBOXVMJMXIYWAETWSAFGBERFQMFETVHUSHF
APSQSFRUCVESHHJAKDFJEFDIESFWJTPPXTZFFEMWVFGALXSGRONRRHAKDRN
```

Frequencies of letters in Ciphertext

```
        X
        X
    XX XX
    XX XXX           X
X   XXXXXX XX  X  XX XX X
XX  XXXXXXXXXXX  XXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXX
ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

Jefferson Wheels

25 wheels,
Key Permutation:
14,7,13,15,1,12,8,16,2,11,17,9,25,3,23,22,4,21,10,20,5,18,19,6,24

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
N	J	E	N	J	L	E	A	L	A	G	L	J	A	G	E	N	G	N	E	L	G	J	A	A
H	P	X	U	G	M	D	L	H	O	U	N	A	B	P	M	V	N	S	L	C	R	I	V	Y
Z	D	B	P	W	D	P	X	O	E	Q	W	K	C	E	W	T	X	W	Z	K	C	Q	Q	S
J	F	O	J	F	Z	O	D	Z	D	W	Z	F	D	W	O	J	W	J	O	Z	W	F	D	D
W	O	P	Z	D	O	Z	Q	Q	X	S	D	W	E	X	T	B	Q	T	W	W	E	K	S	C
K	B	A	K	B	S	A	J	S	J	T	R	V	F	Z	C	Y	T	Y	C	R	Z	V	F	F
E	L	N	E	L	J	N	G	J	G	A	J	L	G	A	N	E	A	E	N	J	A	L	G	G
Q	A	M	V	I	C	F	B	N	Y	P	U	X	H	I	D	H	R	U	X	H	U	P	O	L
D	N	V	X	C	G	Q	P	P	R	L	A	U	I	B	H	M	O	L	U	I	Y	H	N	U
Y	V	C	Y	V	R	C	F	R	F	Z	S	B	J	T	A	K	Z	K	A	S	T	B	J	J
G	X	D	H	P	H	R	H	U	L	I	E	T	K	M	F	Q	U	V	M	N	P	A	Y	B
V	I	L	S	Y	T	M	Y	C	V	R	H	P	L	U	X	U	K	R	I	M	N	G	M	O
F	U	H	M	H	I	G	I	A	U	B	X	E	M	H	Q	D	Y	X	V	P	L	N	R	P
I	T	F	Q	A	N	S	K	E	B	M	Y	M	N	V	R	G	P	H	D	U	I	X	L	H
S	Y	G	F	U	A	L	V	T	I	K	M	G	O	N	I	R	B	D	Q	X	H	E	P	M
M	H	U	L	M	Y	H	U	I	N	Y	P	N	P	L	V	X	V	I	S	G	O	C	K	R
B	K	W	T	Q	K	T	C	W	S	E	Q	O	Q	S	P	Z	C	P	B	O	Q	D	E	X
L	M	R	G	X	U	U	N	Y	H	V	G	C	R	O	S	I	I	Q	F	E	M	T	B	K
P	W	T	B	K	W	B	E	D	C	X	K	Q	S	C	Z	W	E	Z	P	Q	S	O	X	Q
A	R	Y	A	R	B	Y	Z	B	Z	J	V	S	T	F	K	C	J	C	K	V	F	S	T	T
X	C	S	I	T	E	V	R	G	K	O	I	H	U	Y	U	L	M	G	R	Y	V	M	H	N
R	E	Q	D	N	P	I	M	X	P	H	T	Y	V	K	G	F	L	M	H	A	B	U	U	I
O	Z	J	O	Z	F	J	W	F	W	D	F	Z	W	D	J	O	D	O	J	F	D	Z	W	W
T	Q	Z	W	O	Q	W	S	K	Q	C	O	D	X	Q	B	P	S	B	T	D	X	W	C	E
U	G	I	R	E	X	X	O	M	M	N	C	I	Y	R	L	S	H	F	G	T	K	Y	I	V
C	S	K	C	S	V	K	T	V	T	F	B	R	Z	J	Y	A	F	A	Y	B	J	R	Z	Z

Disks are arranged according to the give permutation

14	7	13	15	1	12	8	16	2	11	17	9	25	3	23	22	4	21	10	20	5	18	19	6	24
A	E	J	G	N	L	A	E	J	G	N	L	A	E	J	G	N	L	A	E	J	G	N	L	A
B	D	A	P	H	N	L	M	P	U	V	H	Y	X	I	R	U	C	O	L	G	N	S	M	V
C	P	K	E	Z	W	X	W	D	Q	T	O	S	B	Q	C	P	K	E	Z	W	X	W	D	Q
D	O	F	W	J	Z	D	O	F	W	J	Z	D	O	F	W	J	Z	D	O	F	W	J	Z	D
E	Z	W	X	W	D	Q	T	O	S	B	Q	C	P	K	E	Z	W	X	W	D	Q	T	O	S
F	A	V	Z	K	R	J	C	B	T	Y	S	F	A	V	Z	K	R	J	C	B	T	Y	S	F
G	N	L	A	E	J	G	N	L	A	E	J	G	N	L	A	E	J	G	N	L	A	E	J	G
H	F	X	I	Q	U	B	D	A	P	H	N	L	M	P	U	V	H	Y	X	I	R	U	C	O
I	Q	U	B	D	A	P	H	N	L	M	P	U	V	H	Y	X	I	R	U	C	O	L	G	N
J	C	B	T	Y	S	F	A	V	Z	K	R	J	C	B	T	Y	S	F	A	V	Z	K	R	J
K	R	T	M	G	E	H	F	X	I	Q	U	B	D	A	P	H	N	L	M	P	U	V	H	Y
L	M	P	U	V	H	Y	X	I	R	U	C	O	L	G	N	L	M	V	I	Y	K	R	T	M
M	G	E	H	F	X	I	Q	U	B	D	A	P	H	N	L	M	P	U	V	H	Y	X	I	R
N	S	M	V	I	Y	K	R	T	M	G	E	H	F	X	I	Q	U	B	D	A	P	H	N	L
O	L	G	N	S	M	V	I	Y	K	R	T	M	G	E	H	F	X	I	Q	U	B	D	A	P
P	H	N	L	M	P	U	V	H	Y	X	I	R	U	C	O	L	G	N	S	M	V	I	Y	K
Q	T	O	S	B	Q	C	P	K	E	Z	W	X	W	D	Q	T	O	S	B	Q	C	P	K	E
R	U	C	O	L	G	N	S	M	V	I	Y	K	R	T	M	G	E	H	F	X	I	Q	U	B
S	B	Q	C	P	K	E	Z	W	X	W	D	Q	T	O	S	B	Q	C	P	K	E	Z	W	X
T	Y	S	F	A	V	Z	K	R	J	C	B	T	Y	S	F	A	V	Z	K	R	J	C	G	T
U	V	H	Y	X	I	R	T	C	O	L	G	N	S	M	V	I	Y	K	R	T	M	G	E	H
V	I	Y	K	R	T	M	G	E	H	F	X	I	Q	U	B	D	A	P	H	N	L	M	P	U
W	J	Z	D	O	F	W	S	Z	D	O	F	W	J	Z	D	O	F	W	J	Z	D	O	B	W
X	W	D	Q	T	O	S	B	Q	C	P	K	E	Z	W	X	W	D	Q	T	O	S	B	Q	C
Y	X	I	R	U	C	O	L	G	N	S	M	V	I	Y	K	R	T	M	G	E	H	F	X	I
Z	K	R	J	C	B	T	Y	S	F	A	V	Z	K	R	J	C	B	T	Y	S	F	A	V	Z

Disks are rotated so that the Plaintext appears in a row, then any of the other rows can be used as the cryptotext.

A	B	E	T	T	E	R	B	U	T	M	O	R	E	C	O	M	P	L	I	C	A	T	E	D
B	Y	M	M	U	H	M	L	T	A	K	Z	X	X	D	Q	Q	U	V	V	V	R	Y	P	S
C	V	G	U	C	X	W	Y	Y	P	Q	Q	K	B	T	M	F	X	U	D	P	O	E	F	F
D	I	N	H	N	Y	S	E	H	L	U	S	Q	O	O	S	L	G	B	Q	Y	Z	U	Q	G
E	J	O	V	H	M	O	M	K	Z	D	J	T	P	S	F	T	O	I	S	H	U	L	X	O
F	W	C	N	Z	P	T	W	M	I	G	N	N	A	M	V	G	E	N	B	A	K	K	V	N
G	X	Q	L	J	Q	A	O	W	R	R	P	I	N	U	B	B	Q	S	F	U	Y	V	L	J
H	K	S	S	W	G	L	T	R	B	X	R	W	M	Z	D	A	V	H	P	M	P	R	M	Y
I	E	H	O	K	K	X	C	C	M	Z	U	E	V	W	X	I	Y	C	K	Q	B	X	D	M
J	D	Y	C	E	V	D	N	E	K	I	C	V	C	Y	K	D	A	Z	R	X	V	H	Z	R
K	P	Z	F	Q	I	Q	D	Z	Y	W	A	Z	D	R	J	O	F	K	H	K	C	D	O	L
L	O	D	Y	D	T	J	H	Q	E	C	E	A	L	J	G	W	D	P	J	R	I	I	S	P
M	Z	I	K	Y	F	G	A	G	V	L	T	Y	H	I	R	R	T	W	T	T	E	P	J	K
N	A	R	D	G	O	B	F	S	X	F	I	S	F	Q	C	C	B	Q	G	N	J	Q	C	E
O	N	J	Q	V	C	P	X	J	J	O	W	D	G	F	W	N	L	M	Y	Z	M	Z	G	B
P	F	A	R	F	B	F	Q	P	O	P	Y	C	U	K	E	U	C	T	E	O	L	C	R	X
Q	Q	K	J	I	L	H	R	D	H	S	D	F	W	V	Z	P	K	A	L	E	D	G	H	T
R	C	F	G	S	N	Y	I	F	D	A	B	G	R	L	A	J	Z	O	Z	S	S	M	T	H
S	R	W	P	M	W	I	V	O	C	N	G	L	T	P	U	Z	W	E	O	J	H	O	I	U
T	M	V	E	B	Z	K	P	B	N	V	X	U	Y	H	Y	K	R	D	W	G	F	B	N	W
U	G	L	W	L	D	V	S	L	F	T	F	J	S	B	T	E	J	X	C	W	G	F	A	C
V	S	X	X	P	R	U	Z	A	G	J	K	B	Q	A	P	V	H	J	N	F	N	A	Y	I
W	L	U	Z	A	J	C	K	N	U	B	M	O	J	G	N	X	I	G	X	D	X	N	K	Z
X	H	B	A	X	U	N	U	V	Q	Y	V	P	Z	N	L	Y	S	Y	U	B	W	S	U	A
Y	T	T	I	R	A	E	G	X	W	E	L	H	I	X	I	H	N	R	A	L	Q	W	W	V
Z	U	P	B	O	S	Z	J	I	S	H	H	M	K	E	H	S	M	F	M	I	T	J	B	Q

Transposition Ciphers

A transposition (or permutation) cipher hides the message contents by rearranging the order of the letters.

The Key is a permutation expressed usually as a word or phrase. We assign a number to each letter in the word using the following rule: the numbers are assigned starting with 1, and they are assigned first by alphabetical order, and second, where the same letter appears twice, by position in the word. Thus C R A Z Y B I R D gives the permutation 3 6 1 9 8 2 5 7 4. Key can be a series of numbers as well.

Since a transposition cipher just permutes the letters of a message, at least for long texts, a frequency count will show a normal language profile. Basic idea in cryptanalysis of transposition Ciphers is to guess the period (the Key length), then to look at all possible permutations in period, and search for common patterns. Also lists of common pairs, triples and other features can be used. It is not a good idea to leave message in groups matching the size of the Key.

Rail Fence cipher

The message is written with letters on alternate k rows then the Ciphertext is read off row by row. The number k is called the depth.

Plaintext:

```
BIRDS LOVEW HEATB READB ROWNR ICEAN DAWON DERFU LGRAI NCALL EDQUI NOA
```

Depth 2:
```
B R S O E H A B E D R W R C A D W N E F L R I C L E Q I O
  I D L V W E T R A B O N I E N A O D R U G A N A L D U N A
```

Ciphertext:

```
BRSOE HABED RWRCA DWNEF LRICL EQIOI DLVWE TRABO NIENA ODRUG ANALD UNA
```

Depth 5:
```
B       E       E       R       W       L       L       O
  I     V W     R A     N I     A O     U G     A L     N A
    R   O   H   B   D   W   C   D   N   F   R   C   E   I
      D L     E T     B O     E N     D R     A N     D U
        S       A       R       A       E       I       Q
```

Ciphertext:

```
BEERW LLOIV WRANI AOUGA LNARO HBDWC DNFRC EIDLE TBOEN DRAND USARA EIQ
```

Red Fence cipher

Only difference of this cipher from the rail fence is that the order of the rows in writing the Ciphertext is determined by a Key. Consider the depth 5 rail fence given above.

Key: 34152

Ciphertext:

```
ROHBD WCDNF RCEID LETBO ENDRA NDUBE ERWLL OSARA EIQIV WRANI AOUGA LNA
```

Simple (Row) Transposition Cipher

Write in the message under the Keyword in a number of columns. Then, arrange the columns in numerical order, and write across the Ciphertext.

Key: L O V E B I R D (5 6 8 3 1 4 7 2)

Plaintext

	L	O	V	E	B	I	R	D
	5	6	8	3	1	4	7	2
L	5	B	I	R	D	S	L	O	V
O	6	E	W	H	E	A	T	B	R
V	8	E	A	D	B	R	O	W	N
E	3	R	I	C	E	A	N	D	A
B	1	W	O	N	D	E	R	F	U
I	4	L	G	R	A	I	N	C	A
R	7	L	L	E	D	Q	U	I	N
D	2	O	A						

Columns Permuted

	B	D	E	I	L	O	R	V
	1	2	3	4	5	6	7	8
L	5	S	V	D	L	B	I	O	R
O	6	A	R	E	T	E	W	B	H
V	8	R	N	B	O	E	A	W	D
E	3	A	A	E	N	R	I	D	C
B	1	E	U	D	R	W	O	F	N
I	4	I	A	A	N	L	G	C	R
R	7	Q	N	D	U	L	L	I	E
D	2					O	A		

Ciphertext:
SVDLB IORAR ETEWB HRNBO EAWDA AENRI DCEUD RWOFN IAANL GCRQN DULLI EOA

Key idea for row transposition ciphers is that message is in groups that have the letters reordered in each. Decryption consists of writing the message out in columns and reading off the message by reordering columns. For example, the decryption Key of the above example is 5 8 4 6 1 2 7 3 which is the inverse (permutation) of the encryption permutation 5 6 8 3 1 4 7 2. For ease of recovery, matrix may be completed into a perfect rectangle.

Block (Column) Transposition Cipher

A variant of simple transposition is block (columnar) transposition cipher where the message is written in rows, but read off by columns directly or in order given by the Key.

Plaintext

	L	O	V	E	B	I	R	D
	5	6	8	3	1	4	7	2
L	5	B	I	R	D	S	L	O	V
O	6	E	W	H	E	A	T	B	R
V	8	E	A	D	B	R	O	W	N
E	3	R	I	C	E	A	N	D	A
B	1	W	O	N	D	E	R	F	U
I	4	L	G	R	A	I	N	C	A
R	7	L	L	E	D	Q	U	I	N
D	2	O	A						

Columns Permuted

	B	D	E	I	L	O	R	V
	1	2	3	4	5	6	7	8
L	5	S	V	D	L	B	I	O	R
O	6	A	R	E	T	E	W	B	H
V	8	R	N	B	O	E	A	W	D
E	3	A	A	E	N	R	I	D	C
B	1	E	U	D	R	W	O	F	N
I	4	I	A	A	N	L	G	C	R
R	7	Q	N	D	U	L	L	I	E
D	2					O	A		

Ciphertext (Columns not permuted):
BEERW LLOIW AIOGL ARHDC NREDE BEDAD SARAE IQLTO NRNUO BWDFC IVRNA UAN

Ciphertext (Columns permuted):
SARAE IQVRN AUAND EBEDA DLTON RNUBE ERWLL OIWAI OGLAO BWDFC IRHDC NRE

Decryption consists of calculating the number of rows (by dividing message length by the Key length) and then writing out the message down columns in order given by the Key. For ease of recovery, matrix may be completed into a perfect rectangle.

Nihilist Cipher

A more complex transposition cipher using both row and column transpositions is the nihilist cipher. The message is written in rows then both rows and columns are permuted in order controlled by the Key. Then Ciphertext is read off by rows or columns.

Plaintext

	L	O	V	E	B	I	R	D
	5	6	8	3	1	4	7	2
L	5	B	I	R	D	S	L	O	V
O	6	E	W	H	E	A	T	B	R
V	8	E	A	D	B	R	O	W	N
E	3	R	I	C	E	A	N	D	A
B	1	W	O	N	D	E	R	F	U
I	4	L	G	R	A	I	N	C	A
R	7	L	L	E	D	Q	U	I	N
D	2	O	A						

Columns and rows permuted

	B	D	E	I	L	O	R	V
	1	2	3	4	5	6	7	8
B	1	E	U	D	R	W	O	F	N
D	2					O	A		
E	3	A	A	E	N	R	I	D	C
I	4	I	A	A	N	L	G	C	R
L	5	S	V	D	L	B	I	O	R
O	6	A	R	E	T	E	W	B	H
R	7	Q	N	D	U	L	L	I	E
V	8	R	N	B	O	E	A	W	D

Ciphertext (Read off by rows):

EUDRW OFNOA AAENR IDCIA ANLGC RSVDL BIORA RETEW BHQND ULLIE RNBOE AWD

Ciphertext (Read off by columns):

EAISA QRUAA VRNND EADED BRNNL TUOWO RLBEL EOAIG IWLAF DCOBI WNCRR HED

Diagonal Cipher

The message is written in rows then rows or/and columns are permuted in order controlled by the Key. Then Ciphertext is read off along diagonals. The diagonals can be followed in different directions.

Plaintext

	L	O	V	E	B	I	R	D
	5	6	8	3	1	4	7	2
L	5	B	I	R	D	S	L	O	V
O	6	E	W	H	E	A	T	B	R
V	8	E	A	D	B	R	O	W	N
E	3	R	I	C	E	A	N	D	A
B	1	W	O	N	D	E	R	F	U
I	4	L	G	R	A	I	N	C	A
R	7	L	L	E	D	Q	U	I	N
D	2	O	A						

Columns Permuted

	B	D	E	I	L	O	R	V
	1	2	3	4	5	6	7	8
L	5	S	V	D	L	B	I	O	R
O	6	A	R	E	T	E	W	B	H
V	8	R	N	B	O	E	A	W	D
E	3	A	A	E	N	R	I	D	C
B	1	E	U	D	R	W	O	F	N
I	4	I	A	A	N	L	G	C	R
R	7	Q	N	D	U	L	L	I	E
D	2					O	A		

Rows Permuted

	L	O	V	E	B	I	R	D
	5	6	8	3	1	4	7	2
B	1	W	O	N	D	E	R	F	U
D	2	O	A						
E	3	R	I	C	E	A	N	D	A
I	4	L	G	R	A	I	N	C	A
L	5	B	I	R	D	S	L	O	V
O	6	E	W	H	E	A	T	B	R
R	7	L	L	E	D	Q	U	I	N
V	8	E	A	D	B	R	O	W	N

Columns and rows permuted

	B	D	E	I	L	O	R	V
	1	2	3	4	5	6	7	8
B	1	E	U	D	R	W	O	F	N
D	2					O	A		
E	3	A	A	E	N	R	I	D	C
I	4	I	A	A	N	L	G	C	R
L	5	S	V	D	L	B	I	O	R
O	6	A	R	E	T	E	W	B	H
R	7	Q	N	D	U	L	L	I	E
V	8	R	N	B	O	E	A	W	D

Ciphertext (Columns permuted) Broken Diagonals /:

SVADRRLENABTBAEIEOEUIOWENDAQRBARRANHWIWNDDDOLUCFGLNCLORIAE

Ciphertext (Columns permuted) Continuous Diagonals /:

SAVDRRANELBTBAEIUEOEIOWENDAQNARRABRHWIWNDULODDCFGLOLCNRIAE

Ciphertext (Columns permuted) Broken Diagonals /:

WOONARDILECGBRERIEFAARWLUNIDHLEDNSEEAACLADDAOTQBVBURRIONWN

Ciphertext (Rows permuted) Continuous Diagonals /:

WOONARLIDECGBEIRERFAARWLELHDINUDNSEEADDALCAAOTQBRUBVRIOWNN

Ciphertext (Columns and rows permuted) Broken Diagonals /:

EUDARAIWEASOONAVAFARNDRQNILLENRDGBTDNCCIEUBROWLORBLEHIAEWD

Ciphertext (Columns and rows permuted) Continuous Diagonals /:

EUDAIARWEASAVANOOFARNDRQRNELLINDGBTDNBUEICCROWLOELBRHIAWED

Sacco Cipher

This is a variant of columnar transposition that produces a different cipher. Here, the first row is filled in only up to the column with the Key number 1; the second row is filled in only up to the column with the Key number 2; and so on. Period is k(k+1)/k where k is the length of the Key: the matrix can hold at most k(k+1)/2 letters, so first k(k+1)/2 letters of the Plaintext is encrypted then next k(k+1)/2 letters and so on. Of course, one stops when runs out of Plaintext. After completing the table, the Ciphertext is read off by columns in order given by the Key as in block transposition cipher.

```
 L O V E B I R D
 5 6 8 3 1 4 7 2
---------------
 B I R D S
 L O V E W H E A
 T B R E
 A D B R O W
 N
 R I
 C E A N D A W
 O N D

 E R F U L
 G R A I N C A L
 L E D Q
 U I N O A
```

Ciphertext:
SWODA DEERN HWABL TANRC OIOBD IENEW RVRBN LNALU IQOCE GLURR EIAFA DN

This method has the advantage of dividing the text being transposed in a more irregular fashion than ordinary block transposition.

Transposition Cipher

Plaintext

THEVE RTICE SOFFI VEPLA TONIC SOLID SGIVE THEON LYPER FECTL
YSYMM ETRIC ALDIS TRIBU TIONS OFPOI NTSON THESU RFACE OFASP
HERET HEREF OREIF NPOSI TIVEL YCHAR GEDPA RTICL ESARE CONST
RAINE DTOTH ESURF ACEOF ASPHE REAND NISNO TAPLA TONIC NUMBE
RTHEP ARTIC LESMU STHAV EANEQ UILIB RIUMC ONFIG URATI ONTHA
TISNO TPERF ECTLY SYMME TRICA LITTU RNSOU TTHAT EVENI FNISA
PLATO NICNU MBERT HEEQU ILIBR IUMCO NFIGU RATIO NISNO TNECE
SSARI LYTHE CORRE SPOND INGPL ATONI CSOLI DTHIS ARTIC LEDES
CRIBE SONEE QUILI BRIUM CONFI GURAT IONFO RVALU EOFNU PTOTH
IRTYT WO

Ciphertext

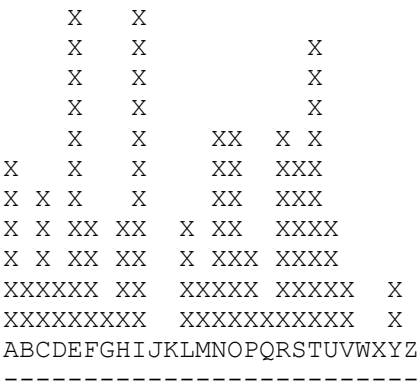
EVCRI THTEE AFLVP SOEFI DIISL TOONC NVOTE SGHIE LETFC LYEPR
CMIER YSTYM UIBTI ALRDS INOOP TIFOS UOSTE NTHSN PCSOA RFFAE
FEEHR HEERT IISNO ORPEF REAYH TICVL LPCRI GETDA TRSCN ESOAE
HNTDO RATIE FROAE ESCUF DHNRA ASEPE ANLTP NIASO EIBNM TOUNC
CEIAT RTRHP VMASH LETSU BEIUL EAINQ GMIOF RINUC ATHOT URNAI
FNRTE TIPSO ELMSM ECYTY UCTLT TRIIA TOATH RNTSU ANSFI EVNEI
UTNNC PLIAO URQHE MBEET OBCIM ILUIR OGIRT NFAIU ENCTE NINSO
ERHLT SSYAI DRNSO COPRE IPNAO INTGL SLIDH CSTOI SIELD ARETC
EBESN CROIE MLUBI QURII TFAGR COUNI UFLRA IOVNO HNTPO EOTFU
XYXWX IROTT

Enciphered using Transposition Cipher.
Using the Permutation 10,4,9,6,8,1,2,7,3,5
The length of the plain tex is 458 letters.

Plaintext alphabet is 26 Letters: A-Z.

```
A B C D E F G H I J
J D I F H A B G C E
```

Frequency in above text: (Each X = 1%)



M-94

Plaintext

THEVE RTICE SOFFI VEPLA TONIC SOLID SGIVE THEON LYPER FECTL
YSYMM ETRIC ALDIS TRIBU TIONS OFPOI NTSON THESU RFACE OFASP
HERET HEREF OREIF NPOSI TIVEL YCHAR GEDPA RTICL ESARE CONST
RAINE DTOTH ESURF ACEOF ASPHE REAND NISNO TAPLA TONIC NUMBE
RTHEP ARTIC LESMU STHAV EANEQ UILIB RIUMC ONFIG URATI ONTHA
TISNO TPERF ECTLY SYMME TRICA LITTU RNSOU TTHAT EVENI FNISA
PLATO NICNU MBERT HEEQU ILIBR IUMCO NFIGU RATIO NISNO TNECE
SSARI LYTHE CORRE SPOND INGPL ATONI CSOLI DTHIS ARTIC LEDES
CRIBE SONEE QUILI BRIUM CONFI GURAT IONFO RVALU EOFNU PTOTH
IRTYT WO

Ciphertext

ZPAHI NIOBN ZCYQO NPEUT FBZZN HUDOK OTGQH JCASY JLTST DTKZI
DVZFQ AANJY PUFZE IQUUY MKHTM GZCSN BKJRY JNBAV HRZNG DYPFC
KPOTU GFTZH TSAEG OAUTE FVIOX MNYKC QJOJT LLDNO NOMXZ HXMJO
DSVQZ LOTUN JUGEJ VQNZP BZKLN ZPFQU FYPBC GUOXZ SNYTZ HLOPK
ABQGU UVDRP BBPKY CCQFP UUKDP VREGX PEYYB NOBHH QXYZZ YKIYO
YQDFX RYGJQ OOCXL FIDFJ SCDRV QXGON VAFFN BALYG SMIJU USMMC
GQMRJ SFRUT CEPIH CYMMF BUPMD XZBPX YSGRO LQBRP AKGCX LIHIX
UOYTC ITAPQ AZVCB VFMYE YKAXR TELKY PFCOQ UVSXJ MIMSQ ICPOJ
LOZHA XYEML HATHZ LOXLR GPTJL DBUVS PBKKB YZBPE APMPY MRFAP
PVOFX ZZA

Enciphered using 'US Army Cipher Device, Type M-94'.
Using the alphabetic Key `'SURFACE'`.
The length of the plain tex is 458 letters.

Plaintext alphabet is 25 Letters: `A-Z, W --> V V.`

Cipher disk order: `15 18 12 9 1 4 7 16 19 13 10 2 5 8 17 20 14 11 3 6`

Frequency in above text: (Each X = 1%)

```
              XX         XX
              XX     X   XX
XXX   X    X  XXXXX   XX  XXX
XXXXXXXXXXXXXXXXXXXXXXX XXX
XXXXXXXXXXXXXXXXXXXXXXX XXX
XXXXXXXXXXXXXXXXXXXXXXX XXX
ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

HAGELIN C-38

Plaintext

```
THEVE RTICE SOFFI VEPLA TONIC SOLID SGIVE THEON LYPER FECTL
YSYMM ETRIC ALDIS TRIBU TIONS OFPOI NTSON THESU RFACE OFASP
HERET HEREF OREIF NPOSI TIVEL YCHAR GEDPA RTICL ESARE CONST
RAINE DTOTH ESURF ACEOF ASPHE REAND NISNO TAPLA TONIC NUMBE
RTHEP ARTIC LESMU STHAV EANEQ UILIB RIUMC ONFIG URATI ONTHA
TISNO TPERF ECTLY SYMME TRICA LITTU RNSOU TTHAT EVENI FNISA
PLATO NICNU MBERT HEEQU ILIBR IUMCO NFIGU RATIO NISNO TNECE
SSARI LYTHE CORRE SPOND INGPL ATONI CSOLI DTHIS ARTIC LEDES
CRIBE SONEE QUILI BRIUM CONFI GURAT IONFO RVALU EOFNU PTOTH
IRTYT WO
```

Ciphertext

```
DSWCX CFNZH FINMA AWWFY HJESY IDCGR WUSFP AJAKV NXENG MQUXP
CNBHQ VELUL LCKRV YLLPG FUKHI MRTDM YXBLG XTWIG ZQZRS OLRYY
QNSJH MADXX FRZMD OFDFF CSAUF CUQQG KQUBA DUPZM UDWWW OHJCB
FWOVR UCJGG TEWLL NOKIV WKLTR WPNKO DMYDI AUINW MMASY IWLMQ
ASPJD THHSJ RPJNZ ZCCQG WUIWI EIIIX SSAIL ZNTLW GGCMS OLDRN
XXVKM YNTHO JOKRQ NSWHJ FIFYX PPAGE ZEIGW SAOBU VEJES SPWZC
BATPM MFVLX HIRHY NBPAA SNSAJ SZBPH AVKPR RNBPL NSEHJ XQWWT
DTNRK GABTS UIFEJ IEFJS ODWLF CUFMM XIJGF GUGME VFDJD OMXYI
UJFQN NHKOP GZPFJ BJDAE XJEVV LXDTF IMLSX ZVSHP UJIKH IMHFV
RZAQD MC
```

Enciphered using 'Hagelin's C-38'.
Using the alphabetic Key '`SURFAC`'.
The length of the plain tex is 457 letters.

Plaintext alphabet is 26 Letters: `A-Z`.

Pin-wheel setup:

```
26 pin wheel:  A b c D e f g h i j k l m n o p q r s t U v W X y z
25 Pin wheel:  a B C D e f g H I j K L m n O P Q R S T U v x y Z
23 Pin wheel:  A b c D E f G h i j k L m n O p q R S T U v x
21 Pin wheel:  A b c d e F G H İ J K l m N o P Q r S t u
19 Pin wheel:  A B c d e f g h i J k L M n O p Q R S
17 Pin wheel:  A B c D E F G h İ J K l M n o p q
```

Lug Positions:

```
Wheel 26:    . . . . . . . . . . X X . . X . . . . . . X . . X . X
Wheel 25:    X X . . X . . . X . . . . . . X X . X X . . . . . . .
Wheel 23:    . . . . . . . . X . . . . . . . . . . . . . X . X X .
Wheel 21:    . . . . X X . X . X . . X . . X X . . X . . . . . . .
Wheel 19:    . . X . . . . . . . . . . . . . . . X . . . . . . . X .
Wheel 17:    . . . X . . . X . . X X X X . . . . . . . X . . X . . .
```

Frequency in above text: (Each X = 1%)

```
X    X  XX  XX    X   X
X  X XXXXX XXX X XX X XX
X XXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXX
ABCDEFGHIJKLMNOPQRSTUVWXYZ
```
